Building Fair Use and Other User Rights into Digital Rights Management

A Thesis
Presented to the Faculty of the Graduate School
of Cornell University
in Partial Fulfillment of the Requirements for the Degree of
Master of Science

by
Amber Sami Kubesch
2014

Building Fair Use and Other User Rights into Digital Rights Management

Amber Sami Kubesch, M.S.

Cornell University 2014

In a fight to protect content from piracy, copyright holders have worked to develop Digital Rights Management (DRM) systems that are harder to break. The result of these stronger measures of protection has been to limit the ways that content can be used and enjoyed by legitimate users, even controlling private performances and displays of digital forms of content. DRM systems make it possible for content owners to limit fair use rights further than allowed under Copyright Law—effectively strengthening these laws in their favor. In addition to the problems with fair use, privacy issues have been raised by DRM technologies that collect user data. This paper begins with a brief overview of how DRM technologies are being used to limit consumer rights. Next it is shown how this code is combined with a legal component, including the use of contractual agreements, to further narrow user rights. Providing a summary of the legal history, it builds up to the current legal environment surrounding DRM in the US. It concludes with my proposal for how DRM policies should be changed to better balance the interests of copyright holders and the public.

Biographical Sketch

I am a student in Electrical & Computer Engineering at Cornell University working with Professor Wicker.

Acknowledgments

I thank Christopher Batten, Professor of Electrical & Computer Engineering at Cornell University, for his continued support and feedback on my research.

Contents

1 Topic Description and Importance

In a fight to protect content from piracy, copyright holders have worked to develop Digital Rights Management (DRM) systems that are harder to break. Robustness against attack is often considered a top priority for DRM designers, as content distributors argue that it only takes one user able to gain unauthorized access to content for it to be illegally shared with many others on the Internet, such as through peer-to-peer file sharing. Some security experts believe that no form of DRM can ever be 100% secure and that attempts to ensure that copying will not happen are futile, while others strive to create more "draconian" systems that make it impossible to circumvent DRM rules [6]. Several DRM experts have argued that users should instead be motivated to accept DRM through the inclusion of value-added components in DRM-protected content to gain consumer acceptance, such as better content delivery, quality, and management as compared to their pirated counterparts.

The trend of DRM, however, is on increasing restrictions, often without offering any intrinsic motivation to accept the technology. The result of these stronger measures of protection has been to limit the ways that content can be used and enjoyed by legitimate users, even controlling private performances and displays of digital forms of content. DRM systems make it possible for content owners to limit fair use rights further than allowed under Copyright Law—effectively strengthening these laws in their favor [1, 22, 28, 67, 68, 70].

In addition to the problems with fair use, privacy issues have been raised by DRM technologies that collect user data. Examples of information collected include the users' system configuration, number of times and timestamps for when the content was accessed, location information, and even very personal data like contact lists; worse, several companies have been found to correlate this data with other user information such as IP addresses, user IDs, gender, and age in order to analyze end users [26, 37, 41, 60, 64, 76, 77]. This process of collecting user data and sending it to remote servers is often done without the knowledge of the user and poses considerable concern.

It has also been discovered that some DRM protections use the same tactics as spyware. In 2005, Mark Russinovich discovered a rootkit on his computer that had been installed from a Sony-BGM audio CD. Subsequent research found that the malware installed even without consent, transmitted information about the user's activities, took steps to both resist detection and removal, and compromised the security of the systems it had been installed on. The included End User License Agreement (EULA) was intentionally vague and misleading about the function of the software, offering only that it was intended to protect the audio files on the CD [25, 31].

While there were sanctions against Song-BGM for their role in the unwanted intrusion of user computers, many other negative components of DRM are supported by the Digital Millennium Copyright Act (DMCA), which prohibits the use or sharing of circumvention tools with some limited exceptions. This means that our ability to exercise fair use rights, protect our privacy, and enjoy other consumer rights that we were once able to take for granted are at risk. We cannot count on content distributors to be honest, considerate, accountable, or transparent; instead we must seek to rebuild a framework under which the rights of users can be reclaimed and balanced against the needs of content providers.

This paper begins with a brief overview of how DRM technologies are being used to limit consumer rights. Next we show how this code is combined with a legal component, including the use of contractual agreements, to further narrow user rights. Providing a summary of the legal history, we build up to the current legal environment surrounding DRM in the US. We conclude with our proposal for how DRM policies should be changed to better balance the interests of copyright holders and the public.

2 Code Context

To show why there is a pressing need for a form of DRM that incorporates fair use and other consumer rights, we share several ways in which DRM currently imposes on these rights. In addition to the limitation or removal of many fair use rights, we look at other actions taken through DRM by content distributors, such as invalidating or removing access to purchased content, retroactively restricting DRM privileges after purchase, the reduction of user privacy by collecting and sending personal information through processes that "phone home," and some malware-like tactics used by DRM coders to control users' systems.

One issue with DRM protected content is that of renewability, or the ability to delete or alter features after purchase. An ebook seller, Fictionwise, used a third-party supplier of DRM encrypted ebooks, Overdrive, to supply approximately 300,000 electronic book titles to its users. Providing only 30 days of warning to customers, Overdrive's servers were shut down on January 30, 2009. The files already downloaded continued to work but the purchases were invalidated, removing the ability of users to transfer content to a new device or obtain a replacement if the original file was lost or deleted. Fictionwise stated in their FAQs online that "Fictionwise strives to maintain your purchases indefinitely, but our terms of service do not guarantee they will be available forever. Forever is a long time. [...] We do not have legal control of those third party servers. If those third party servers 'go dark' for one reason or another, we have no way to continue delivering those files. It is important

to note that other ebook retailers such as Barnes and Noble, Gemstar, and Amazon.com's original ebook store circa 2004 did not make any effort to maintain long term customer access to purchased material when they shut down their ebook operations in the past. They announced a time period for final download then shut down the servers" [15, 21, 71].

Ebook users faced another issue with renewability when Amazon deleted copies of George Orwell's *1984* and *Animal Farm* as well as some works of Ayn Rand from users' Kindles, rendering user-added notes and annotations associated with those files useless [69, 71]. Amazon refunded the purchases, but left users angry that the company had the ability to retroactively modify user access to purchased content.

Short of removing entire works, some users experienced changes in DRM privileges after purchasing content. The Author's Guild fought to force Amazon to block text-to-speech privileges on a title-by-title basis from the Kindle [5], and Amazon ultimately agreed to remove the functionality from already purchased titles on users' devices at the request of publishers [71].

This issue is not confined to ebooks; consumers of music and video games have faced similar losses. In 2008, music services offered by MSN, Yahoo! Music, and Walmart Music announced that they would be shutting down their DRM servers and that users would no longer be able to transfer songs to new devices or access purchased content after changing operating systems. Customer reactions caused MSN and Walmart to announce a delay in their shutdown date and Yahoo! to offer compensation to their customers [15]. Users of Apple's iTunes service also experienced DRM privilege restrictions. Prior to April 2004, the iTunes music store allowed users to burn purchased music on up to 10 CDs. Apple later issued an update to iTunes reducing that limit to only 7 allowable copies [14]. In another case, Epic Game's Gears of War software came with a digital certificate that expired on January 28, 2009, about three years after the game was released. Users who had legally purchased the game became unable to use the product until the creators fixed the certificate (or until they realized that changing their system clock tricked the game into registering the certificate as still valid). Ironically, users with a pirated copy of the game did not have this problem [15, 17].

Another consumer cost of DRM is loss of privacy. DRM has "the potential to facilitate an unprecedented degree of surveillance of consumers' reading, listening, viewing and browsing habits" [6]. This may be even more intrusive in the mobile realm, where "smartphones are often on and tethered to their user, transmitting rich data to the app developers. Users of mobile devices are vulnerable to privacy intrusion and abuse by numerous entities, app developers, analytic services and advertising networks. These entities could have access to sensitive information, including a user's location, con-

tacts, identity, messages and photos" [56]. A Wall Street Journal Investigation on the topic found that "these phones don't keep secrets. They are sharing this personal data widely and regularly" [77].

In fact, some users reported to have run tests discovering that several Pinch Media enabled iPhone apps were storing and sending back to Pinch Media's servers ("phoning home") combinations of the following data: a unique device identifier, iPhone model, OS version, app version, if the iPhone running the app was jailbroken, if the copy of the app had been pirated, the times and dates when the app was opened and closed, latitude and longitude of the iPhone, and—if Facebook enabled—the gender, birth month and day of the user [41, 60]. Flurry Analytics, which has since merged with Pinch Media, admits in their privacy policy that they collect the following data: "User ID (for your service), latitude and longitude (obfuscated by Flurry to state/city), gender, age, events, errors, and page views. Finally, we see the IP address, device type, locale and timezone of the user through the HTTP request. [...] In addition, we may provide you with the option of exporting raw Flurry data to your servers such as timestamp, platform, event, and user ID" [26]. Co-founder of Pinch Media, Greg Yardley, responded to outrage over the discovery that Pinch Media-enabled apps were phoning home by saying, "Every single person who installs an iPhone application consents to data collection in advance—it's right there in the default EULA Apple's provided so developers don't have to hire lawyers before publishing something," defending that "There's always a subset of people who don't care how useful analytics are, and automatically object to any analytics-providing company. Some don't get how analytics make a lot of what they enjoy possible [...] Some do understand this, but don't think it's worth the price of privacy. That's an honest opinion, and we'll have to [respectfully] disagree, although I wonder why such a person would even have a mobile phone to begin with, since the carriers track things much more personal than we ever will, and are much more likely to share them"[1].

While many times not transparent to users, these activities may indeed be allowed by the EULA, although often in vague, non-limiting terms. There are many other analytics companies like Flurry, including Medialet and Mobclix, but it's often not known to users that some of their apps are running analytics software, which ones are collecting this data, or the scope of data being obtained [37, 53, 54, 77].

Although analytics companies defend this process as one in which no personally identifiable information is collected, the practice of collecting a device's unique identifier means that they are able to

[1]This quote from Greg Yardley was originally found as a comment to an article posted online at *http://gadgets.boingboing.net/2009/04/13/pinch-media-statisti.html#comment-463496)*. I verified with him via email communication on November 12, 2013 that it was his comment.

track users over time. Unlike cookies, this is built into the device and cannot be cleared [77, 88]. One user wrote in response to Pinch Media that "As far as not having personally identifiable information, the fact is that as soon as I use an app that requires registration of my name or email address, then my [unique device identifier (UDID)] could be associated with my identify by the developer of this app. What's to stop you from gathering this information from developers? Even if you don't have my name, the [(UDID)] might as well be my name" [41].

Apps like Facebook, Hipster, and Path, and about a dozen others were found to be uploading user's contact lists to their servers in a move later defended by Path as being an industry-standard practice [33, 34, 55, 64, 76, 88]. Seven popular mobile games created by Storm8 were also criticized for sending home users' phone numbers, unique device identifiers, and email addresses, all unencrypted in plain text. [7, 29]. Programs downloaded from an app store are not the only ones potentially collecting user data, however. One developer discovered that the WebOS side of his Palm Pre device "periodically uploads information to Palm, Inc" [32], including location data and application usage. Carrier IQ, software installed on 150 million phones by cell phone companies, was found to be recording keystrokes, location data, browsing history, application use, battery use, and radio activity [12, 13]. Possibly the result of an error, it was also found "that keystrokes, text message content and other very sensitive information is in fact being transmitted from some phones on which Carrier IQ is installed to third parties" [12].[2] Finally, while users may feel comfortable and let their guard down when using iPhone's Siri feature, they should keep in mind that it collects user data in order to have a better context for the spoken commands and that Apple reserves the right to retain both voice inputs and user data for their own uses as well as those of their subsidiaries [2].

Along with contact lists, it is also possible for mobile apps to access and copy entire photo albums without the user's knowledge or explicit opt-in, as found on both Apple and Android devices [8, 9]. In addition, Black Hat researcher, Nicolas Seriot, developed a proof-of-concept iPhone app that was able to collect and send home the following data: phone number, address book contents, recent Safari searches, YouTube history, email account data including full name and email address, unique device identifier, SIM card serial number, and International Mobile Subscriber Identity [72]. Spyware under the name of FinFisher was found to be able to "secretly turn on a device's microphone, track its

[2]Security researcher Trevor Eckhart, who discovered the Carrier IQ rootkit software, was sent a Cease & Desist notice from Carrier IQ citing copyright infringement and demanding "that Eckhart turn over contact information for every person who had obtained the files from him, and that he replace his analysis with a statement—written for him by Carrier IQ—disavowing his research" [39]. Ultimately the Electronic Frontier Foundation took up his case and concluded "that Carrier IQ's real goal [was] to suppress Eckhart's research and prevent others from verifying his findings," one risk of abuse of the Digital Millennium Copyright Act.

location and monitor e-mails, text messages, and voice calls" [73] on a range of mobile devices including the iPhone and BlackBerry.[3] While these examples show what technology is currently possible in the realm of mobile devices, these activities may be illegal based on current EULAs. However, it raises the question of how far companies could take the terms in their user agreements. Certainly a line must be drawn beyond which courts in the US would consider such terms to be unreasonable, unconscionable, and ultimately illegal.

The phenomenon of protected content collecting personal data and "phoning home" isn't limited to mobile apps. In 2005, it was discovered that Song-BMG's copy-protected CDs were transmitting personal information without the user's knowledge or consent [31]. Specifically, the DRM systems implemented by Song-BMG "were designed to contact a vendor Web site whenever the user inserted a protected disc. The ostensible purpose of this was to download images or advertisements that would be displayed while the music played, but it also created entries in the vendor's Web server log, noting the users' IP addresses, disc inserted, and the times and dates it was inserted" [25].

On top of this, the discs performed undisclosed installation of software onto consumer's computers. The discs shipped with two versions of DRM, one called XCP (extended copy protection) another under the name of MediaMax. XCP was a rootkit that cloaked its presence by modifying the system to hide the fact that it was running and to make it challenging to remove. The MediaMax version also resisted detection and removal, installing itself even if the user declined the terms in the EULA. Researchers Halerman and Felten concluded that their case study on Song-BMG revealed "similarities between DRM and malicious software such as spyware, the temptation of DRM vendors to adopt malware tactics, the tendency of DRM to erode privacy, the strategic use of access control to control markets, the failure of ad hoc designs, and the force of differing incentives in shaping behavior and causing conflict" [31]. Another researcher pointed out that "Even if Sony BMG disclosed the existence of this software in the End Users' License Agreement (EULA), the agreement did not disclose the real nature of the software being installed, the security and privacy risks it created, the practical impossibility of uninstalling and many other potential problems for the user's computer" [50].

The third complaint with the tactics used by Song-BMG was that of limited portability. After purchase, users learned that they were limited by the number of digital copies of the material that they could create, that they had to use Sony's proprietary media player to play the content on their computers, and that they weren't permitted to convert music to common digital formats such as that used by iTunes. Ultimately this meant that the files were only compatible with Sony and Microsoft

[3] This is not just a worry for the future; some Android and iPhone apps from their respective app stores have already been found to secretly activate cell phone microphones, including *Color*, *Shopkick*, and *IntoNow* [16, 64].

portable players and unusable with other devices like the iPod.

The investigations of Song-BMG copy-protected disks revealed several ways in which content owners do not make limitations transparent to users before purchase. Here, consumers were only made aware of portability issues after inserting the disks into their computers and were unaware that Sony's media player would be serving advertisements while they played their paid content [50].

Consumers of ebooks also often do not know what limitations they will face until after they have purchased the content. They may be surprised to learn that features such as read-aloud and use with third party programs can be disabled on a title-to-title basis. While this may be a minor inconvenience to some users, it could be a big problem for those with disabilities who rely on those features in order to make use of the content, such as users who need the use of an included read-aloud function or the ability to interface with third party software that can do so [71]. "The advent of digital technology makes it easier than ever for disabled people to enjoy the same media as people without disabilities. A digital book can be read aloud by a blind user's computer, sparing her the need to wait until [a] volunteer can be found to record an audio version. Indeed, for the first time the blind can enjoy newspapers at the same time as the sighted, simply by 'reading' them through a Web-browser that reads the articles aloud to them, or exports them via a Braille terminal. [...] However, DRM systems stymie these activities. Adobe's ebooks come with the capacity to be read aloud by a computer, but allow authors to switch this capability off. Other ebook technologies lack this capability altogether, and actively prevent interoperability with third party software such as text-to-speech programs" [14].

DRM code is able to limit access and interoperability, locking consumers out of expected functionality or that which could be offered through third-party vendors. "In a few words, the restrictions imposed by technological measures are frequently unclear to consumers. This lack of information can induce consumers to make buying decisions which they would not have made had they been better informed" [50]. In order to maintain fairness where DRM is used, these limitations should be disclosed before purchase to enable consumers to make informed buying decisions.

Digital restrictions like these combined with anti-circumvention legislation have been criticized for limiting or removing fair use rights. Passed in 1998, the Digital Millennium Copyright Act (DMCA) made the circumvention of copyright protection mechanisms illegal, with the temporary exception of a limited number of classes of works [48, 82]. One effect of the DMCA has been to narrow fair use rights further than the provisions (otherwise) made in law for copyright holders. Succinctly, "Copyright owners can effectively eliminate fair use by utilizing DRM systems sanctioned under the DMCA and litigating against anyone who tampers with those measures. Thus, re-writing the copyright

fundamentals developed by Congress and courts over more than a century" [70].

One harm of this can be seen in the area of scholarly research. For example, while motion picture excerpts can now legally be obtained through DRM circumvention for the purpose of commentary, criticism, or educational uses in accordance with the most recent DMCA exemptions[4], there are still many other possible educational purposes for circumvention of technological barriers that are not permitted [48]. This includes the loss of ability to digitally analyze protected content, such as using third-party software to search and analyze text in books, thematic searches of musical scores, or analyses of computer programs [1].

3 Legal Context

In this section, we show examples of terms being included in EULAs such as those prohibiting users from engaging in class-action lawsuits, requiring that users allow collection of their personal data, and even those that force users to relinquish fair use rights. Several case studies in the US are presented and compared to the way similar agreements are being handled in the European Union (EU). The EU has established some fundamental consumer rights and taken action against companies that require EULAs with unconscionable terms; in the US, although several legal attempts have been made to limit the ability of contractual agreements to force users to waive rights they would otherwise have enjoyed under copyright law, we have not seen the same success in this area as Europe. To establish the current legal atmosphere surrounding DRM and user agreements, current and failed bills on the topic are presented. Finally, a comparison is made showing the overarching differences guiding privacy protection and data flow legislation for members nations of the European Union to those in the Asia-Pacific Economic Cooperation (APEC), the latter of which includes the United States.

The current legal environment in the US is perceived by many to be skewed unfairly in favor of copyright holders. In addition to the code-based restrictions imposed on users by DRM technology, further rights can be taken away through licenses and contracts, such as End User License Agreements (EULAs) [11, 14, 15, 28, 49, 51, 67, 68, 70].

[4]There is a catch to the DMCA exemptions, however; they are only valid for a period of three years, at which time some can be renewed but there is no guarantee. In the words of the Copyright Office, Library of Congress, "In each rulemaking proceeding, the Register and Librarian review the proposed classes de novo. The fact that a class previously has been designated creates no presumption that redesignation is appropriate. While in some cases earlier legal analysis by the Register may be relevant to analyzing a proposed exemption, the proponent of a class must still make a persuasive factual showing with respect to the three-year period currently under consideration" [48].

As of this writing, some EULAs include terms to prohibit users from participating in a class-action lawsuit or to require users to allow collection of their personal data. Consenting to the Sony Playstation Vita System of Software License Agreement (Version 1.1) [74] or the most recent PayPal User Agreement [62], for example, means that the user waives the right to engage in a class-action lawsuit against the company—unless a written notification requesting the retention that right is sent within 30 days of accepting the agreement. Facebook retains the right to log and use data on users including the IP address, date, and time of all logins and logouts; messages sent between users; a history of conversations through Facebook Chat; all notifications and whether the user had email and text enabled or disabled for each; any photos uploaded to a Facebook account (presumably even those later deleted); as well as a history of other sites visited. Facebook is only one of many services that collect user data. The iTunes 10.7 license agreement, for example, states that "If you opt in to diagnostic and usage collection, you agree that Apple and its subsidiaries and agents may collect, maintain, process and use diagnostic, technical, usage and related information, including *but not limited to* information about your computer, system and application software, and peripherals, that is gathered periodically" [3] (emphasis added). Users are opted in by default, and what a user must to do to opt out is not immediately clear or disclosed in the agreement.

The Electronic Frontier Foundation warns that "Companies have a lot of leeway about what goes into the privacy policy. They can use vague, overbroad language so they can collect lots of data about users, share it with affiliates, sell it to marketers, or provide it to the government upon request. And even a strong privacy policy is little consolation; a privacy policy can change at any time, so today's protective language could be tomorrow's permissive exceptions" [38]. Considering that most Americans believe that their information is being kept private when they see the term "privacy policy" [78], that the common attitude of consumers toward EULAs is to select that they agree without reading the terms [88], and that the terms in these contracts are unilaterally determined and dictated, users today find themselves in a very poor position with respect to the companies drafting these license agreements.

The European Union has established some fundamental consumer rights and taken action against companies that require EULAs with "unconscionable" terms. Some terms that have been argued to be unfair include those that allow the copyright holder to modify the agreement without notice, to change the rights restrictions on already purchased files, to limit interoperability with other software or devices, to disclaim responsibility for any viruses or other damage that could result to the user's computer system through use of their services or products, as well as other misleading or unfair behavior including terms users likely would not have accepted had they understood what was included

[27, 50].

In the U.S. however, EULAs in the form of click-through or shrink-wrap agreements are being upheld in courts (although not consistently). A high profile case illustrating this was that of Blizzard vs. bnetd.org. Vivendi-Universal's Blizzard Entertainment alleged that software created by bnetd.org allowing users to play Blizzard games over the Internet was only made possible by the defendant's use of reverse engineering, a violation of Blizzard's ELUA. A court ruled in 2005 that even if this would have fallen under fair use, bnetd.org waived that right by agreeing to Blizzard's ELUA [15, 83].

Even though some legal attempts have been made to limit the ability of contractual agreements to force users to waive rights they could have otherwise enjoyed under Copyright Law, the U.S. has not seen the same success in this area as Europe. In 1997, Rep. Boucher introduced the Digital Era Copyright Enhancement Act (105th Congress Bill H.R. 3048) to Congress as an alternative to the restrictive proposals under the DMCA; however, it died after being referred to a subcommittee in 1998, ultimately losing out to the DMCA proposal. Some of the major differences between H.R. 3048 and the DMCA include that the former took fair uses into consideration by only prohibiting the alteration or removal of DRM restrictions when done for the purpose of infringement. Further, H.R. 3048 would have prohibited the ability of copyright owners to limit fair use rights through shrink-wrap or click-through agreements [6, 46, 47].

Another bill proposed to establish greater consumer rights with respect to DRM, The Consumer, Schools, and Libraries Digital Rights Management Awareness Act of 2003, was introduced by Senator Brownback and supported by the U.S. Public Policy Committee of the Association for Computing Machinery (USACM). Among the terms proposed were to promote greater public transparency when DRM is used to protect digital content, greater privacy rights for users, and prohibitions on the government from mandating the use of any specific copy-protection technologies. This bill also died in Congress.

"Pro-digital-consumer legislation has enjoyed no great success in U.S. The most famous consumer-rights legislation proposed in the recent time, the Digital Media Consumers' Rights Act (DMCRA), has been introduced into Congress three times without success" [50]. First introduced in 2003, the goals of DMCRA were to restore fair use rights to users by allowing the circumvention of copy protection measures for the purpose of scientific research or when "such circumvention does not result in an infringement of the copyright in the work" [44]. It would have also allowed the distribution of hardware and software enabling such circumvention if there existed a "significant noninfringing use" for the technology. It would have also required greater transparency of limitations through the clear labeling

of copy-protected compact discs.

Nations take different approaches to privacy protection, ranging from a "strong 'rights-based' approach [as] embodied in the [EU] Data Protection Directive, to the US preference for relying on market forces rather than the law to protect personal information" [49]. The United States is one of 21 member economies of the Asia-Pacific Economic Cooperation (APEC) that have agreed to the APEC Privacy Framework in order to create region-wide compatibility of privacy policies and data flow [4]. "The significance of the twenty-one APEC economies adopting common information privacy standards cannot be doubted. The APEC economies are located on four continents, account for more than a third of the world's population, half its GDP, and almost half of world trade" [30].

One complaint with APEC Privacy Framework is that it allows collected data to be used for any "compatible or related purposes" and does not suggest that collection should be the least necessary. Although APEC member nations can implement stronger regional laws, doing so seems to be discouraged: the forward to the Framework states that "Member Economies, consistent with the APEC Privacy Framework and any existing domestic privacy protections, should take all reasonable and appropriate steps to identify and remove unnecessary barriers to information flows and avoid the creation of any such barriers" [4]. Showing a preference for allowing data flow over protecting privacy, "The Preamble speaks of 'ensuring' free flow of information but only of 'encouraging' privacy protection. The final points in the Preamble refer to free flow of information as 'essential', but do not accord this status to privacy protection. These examples of terminology indicate how the Framework has a bias against privacy protection in favor of free flow of information" [30].

4 Recommendations for Improving DRM Design

We propose several changes for DRM systems and expand on basic principles of good DRM design.

(1). Copyright Balance: In line with the idea that DRM should only be used to reinforce existing copyright laws and not to add further restrictions, we recommend a starting point for which fair use rights and copyright protections can be balanced.

With copyright holders having a possible conflict of interest with fair use rights, they should not be in charge of determining if access should be blocked through the use of DRM. "A fair use is by definition unauthorized and therefore does not require interaction with or compensation to the copyright holder. Indeed, many legitimate fair uses, including criticism, commentary, news reporting, teaching, scholarship, and research, might well conflict with the interests of the copyright holder" [18]. A minimal level of access then should be required of DRM for fair use rights.

The United States Copyright Offices lists the following four criteria as those used to make fair use determinations: "(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work" [80]. This vague nature of fair use makes it a legal gray area and difficult, if not impossible, to translate into code [22]. However, rather than allowing copyright holders the option to eliminate these rights, previous legal cases should be used to establish reasonable boundaries within which DRM should operate. Focusing on the quantitative component of the third criterion used to determine fair use, we looked at summaries of legal cases involving fair use to calculate the percentage of overall content taken from the copyrighted work. Based on cases where it was possible to assign a percentage to the amount of the content used [75, 84, 85], we recommend that a minimum of 1% of text, audio, and video be made available through DRM for copying purposes. Note that this 1% recommendation would not imply that any use of that amount of material would fall under fair use (or that any greater percentage would not), but rather to serve as a starting point for finding a reasonable balance between adequate content protection and better access to fair use rights.

We also seek to have DRM coders include expirations for their protections that correspond with copyright expirations; this will ensure that public domain works are not unfairly limited by (possibly no longer supported) DRM technologies.

(2). Privacy: Although some data collection is needed to complete transactions, the collection, storage, and redistribution of personal information should only be allowed as is necessary for the proper functioning of the DRM system. Further, user agreements should not require users to relinquish privacy when the data is not necessary for the DRM system. Based on principles of privacy-aware design [92], we suggest that DRM adheres to the following framework: DRM systems provide a full disclosure of data collection, users must first consent to any data collection through acknowledgments and opting-in, the amount of personal data collected is minimal and only taken when there is a functional requirement to do so, the identification of data with individuals is minimized, and data is stored only when there is a functional requirement for its retention.

At minimum, DRM must adhere to the following guidelines when data collection is involved: maintain transparency, only use data in the context within which it was collected, provide an ability for users to access and amend personally identifying data, provide the option to permanently delete data when a user wants to leave a service, securely handle and store data, and respect reasonable limits on what is appropriate to collect [20, 35, 37, 40, 43, 57, 88].

- Transparency: A final commission report issued by the Federal Trade Commission (FTC) advocates for better transparency for users. They urge that "Companies should increase the transparency of their data practices; privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices; companies should provide reasonable access to the consumer data they maintain and the extent of access should be proportionate to the sensitivity of the data and the nature of its use; and all stakeholders should expand their efforts to educate consumers about commercial data privacy practices" [20]. Users should be made aware of exactly what data is being accessed, how long the data will be stored, how the data will be used, and where the data will be shared [35, 43].
- Respect for Context: The Electronic Frontier Foundation suggests that "Applications that collect data should only use or share that data in a manner consistent with the context in which the information was provided. If contact data is collected for a 'find friends' feature, for example, it should not be released to third parties or used to e-mail those contacts

directly. When the developer wants to make a secondary use of the data, it must obtain explicit opt-in permission from the user" [35].

- Right to Access and Amend: "There must be a way for a person to correct or amend a record of identifiable information about the person" [43].
- Right to Delete: "Particularly where privacy tradeoffs have not been made clear, consumers need the ability to change their minds and walk away from a service. While the Federal Trade Commission has so far focused upon improving consumers' positions ex ante, increasingly we need to consider ex post interventions, such as a right to delete information associated with an account, so that the consumer can exit whole" [88]. In the case of social media, "A user should have the right to delete data or her entire account from a social network service. And we mean really delete. It is not enough for a service to disable access to data while continuing to store or use it. It should be permanently eliminated from the service's servers" [57].
- Security: An FTC report found that "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data. These harms may include the unexpected revelation of previously private information, including both sensitive information (e.g., health information, precise geolocation information) and less sensitive information (e.g., purchase history, employment history) to unauthorized third parties" [20]. To protect users, data should be encrypted whenever possible, [37] including during transit, during storage, against external attacks, and "against the threat of employees abusing their power to view sensitive information" [35].
- Limitations: "Consumers have a right to reasonable limits on the personal data that companies collect and retain" [40]. EULAs should not be used to take advantage of consumers and allow data collection that users would not want to share.
- Privacy by Design: "Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services; companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy; and companies should maintain comprehensive data management procedures through the life cycle of their products and services" [20].

There would need to be a legal component in order to gain compliance, as it is not always in a company's best interest to provide this level of privacy. A UC Berkeley Law study found that

"Even when companies know that consumers want more privacy, firms can have incentives to code in privacy-invasion options by default. Firms may also have incentives to hide the tussle" [88].

(3). Consumer Protection: In addition to fair use rights, DRM should not be used to restrict other user rights or to disadvantage consumers. This includes prohibiting unconscionable terms in user agreements, requiring transparency for DRM restrictions before the sale of content, and demanding accountability. Currently, many consumers cannot determine which actions will be permitted while using a specific digital content (such as read-aloud for an ebook) until after the purchase has been completed, putting consumers in a poor position with respect to the content distributors.

- Renewability: Manufacturers/suppliers should not be allowed to further narrow rights of consumers post-purchase [65, 71].
- Transparency: "Consumers must be able to judge the quality and characteristics of complex technological products and services. There is little doubt that disclosure and transparency are effective means of protecting their rights and interests, especially in cases of information asymmetry" [50].
- Accountability: Developers should be responsible for the hardware and software they create, including any possible harm that may result from using the content or device [37]. To increase accountability, exemptions should be granted through the DMCA for security research and compliance validation.

As copyright holders are not inherently interested in preserving these rights, as shown by current market trends, legal policies would need to be established to monitor DRM and contractual agreements in order to protect consumers.

(4). Competition:

The Electronic Frontier Foundation (EFF) has argued that some DRM-based technologies—such as DVD Players—do little to ensure protection of the content; they make the argument that DRM here is being used more to eliminate competition than piracy [14,15]. The EFF points out that some of the DVD Content Control Association's (DVD-CCA) technologies, such as CSS, have been cracked for years. Through licensing agreements though, the DVD-CCA is able to

require innovators seeking to implement new features for DVDs to first gain permission through a negotiation process involving movie studios and big computer companies.[5]

Some copyright holders are able to use licensing agreements to maintain control over technologies, limit interoperability, and thus limit competition. To solve these issues, public policy needs to be adapted to encourage better interoperability among the various DRM approaches and to enable more competition.

(5). Research and Public Discourse: DRM systems and the laws that protect them should not interfere with non-infringing scholarship, as doing so impedes scientific progress. An example of this impact on the academic community was seen when the Secure Digital Music Initiative (SDMI) forbid the publication of a paper by Felten et. al. that revealed weaknesses in the watermarking standards proposed by the former. SDMI claimed that the paper was an illegal circumvention technology, forcing Felten to seek a court decision in order to allow the publication. To avoid similar threats, he used the legal advice of several attorneys while working on a later publication, writing that "sadly, research of this type does seem to require support from a team of lawyers" [31].

Although the DMCA has offered exemptions for specific categories of encryption research and security testing—allowing legal circumvention for some researchers—these relaxations in the DMCA regulations were limited and in effect for only three years; at the conclusion of that time, the Librarian of Congress makes new determinations, providing no guarantees of continuing to protect these classes of scholarship. Additionally, not all types of academic research have been granted exemptions. Circumventing DRM for the purposes of thematic searches and analysis of musical scores or word frequency analysis, for example, have not been granted the same privileges.

5 Conclusion

DRM is used to mitigate the losses content owners face due to piracy, but this technology also enables copyright holders to overreach their rights and narrow those of consumers. The current legal and technological landscape shows that we cannot rely on market forces alone to find a fair balance

[5]The interested reader is encouraged to learn more about actions taken by the DVD-CCA against Kaleidescape and RealNetworks by looking at E. Bangeman, *DVD Licensing Group to Vote on Closing Copying Loophole*, http://arstechnica.com/uncategorized/2007/11/dvd-licensing-group-to-vote-on-closing-copying-loophole/ (Nov. 5, 2007) and G. Sandoval, *RealNetworkds Set to File Appeal in RealDVD Case*, http://news.cnet.com/8301-31001_3-10369812-261.html (Oct. 7, 2009).

between the rights of users and those of copyright holders. We encourage legislators to safeguard users rights by developing a legal backing for the recommendations presented in this paper. We also encourage developers of DRM to remain mindful of these suggestions and to carefully consider the impact their technology has on consumer rights, including fair use and privacy.

References

[1] A.W. Appel and E.W. Felten. "Technological Access Control Interferes with Noninfringing Scholarship." *Communications of the ACM*, 43(9), September 2000.

[2] Apple, Inc. "iOS Software License Agreement (EA0930)." 8 October 2012. Web. 1 March 2013. <http://www.apple.com/legal/sla/docs/ios6.pdfâĂŐ>.

[3] Apple Inc. "Software License Agreement For iTunes." August 23, 2012.

[4] Asia-Pacific Economic Cooperation. "APEC Privacy Framework." 2005. Web. 7 August 2013. <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/ /media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx>.

[5] The Author's Guild. "Amazon Reverses Stance on Computer-Generated Audio for the Kindle 2." 2 March 2009. Web. 10 October 2012. <http://www.authorsguild.org/advocacy/articles/amazon-reversal-on-text-to-speech.html>.

[6] E. Becker, W. Buhse, D. Günnewig, and N. Rump. Digital Rights Management: Technological, Economic, Legal and Politcal Aspects. *Springer*, 2003.

[7] Y. Benjamin. "Apple Privacy Score: Snow Leopard - 10, iPhone - 0." SFGate. 27 August 2009. Web. 9 November 2013. <http://www.sfgate.com/cgi-bin/blogs/ybenjamin/detail?blogid=150&entry_id=46236>.

[8] N. Bilton. "Apple Loophole Give Developers Access to Photos." The New York Times. 28 February 2013. Web. 8 November 2013. <http://bits.blogs.nytimes.com/2012/02/28/tk-ios-gives-developers-access-to-photos-videos-location/>.

[9] B.X. Chen and N. Bilton. "Et Tu, Google? Android Apps Can Also Secretly Copy Photos." The New York Times. 1 March 2012. Web. 10 November 2013. <http://bits.blogs.nytimes.com/2012/03/01/android-photos/>.

[10] D.S. Chisum, T.T. Ochoa, S. Ghosh, and M. LaFrance. Understanding Intellectual Property Law (2nd Edition). *LexisNexis*, 2011.

[11] J.E. Cohen. "DRM and Privacy." *Communications of the ACM*, 46(4), April 2003.

[12] P. Eckersley. "Some Facts About Carrier IQ." Electronic Frontier Foundation. 13 December 2011. Web. 8 November 2013. <https://www.eff.org/deeplinks/2011/12/carrier-iq-architecture>.

[13] T. Eckhart. "CarrierIQ" Android Security Test. Web. 8 November 2013. <http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/>.

[14] Electronic Frontier Foundation. "Digital Rights Management: A Failure in the Developed World, a Danger to the Developing World." Web. 15 September 2012. <http://w2.eff.org/IP/DRM/drm_paper.php>.

[15] Electronic Frontier Foundation. "FTC Town Hall: Digital Rights Management Technologies." March 2009. Web. 13 October 2012. <www.eff.org/files/filenode/DRM/DRMCOMMENTS_final.pdf>.

[16] M. Elgan. "Snooping: It's Not a Crime, It's a Feature: New Apps Hijack the Microphone in Your Cell Phone to Listen in on Your Life." 16 April 2011. Web. 12 November 2013. <http://www.computerworld.com/s/article/9215853/Snooping_It_s_not_a_crime_it_s_a_feature>.

[17] Epic Games. Gears of War Official Forums. Web. 13 October 2012. <http://forums.epicgames.com/threads/656177-quot-You-cannot-run-the-game-with-modified-executable-code-quot-WTF-help-please!/page3>.

[18] J.S. Erickson. "Fair Use, DRM, and Trusted Computing." *Communications of the ACM*, 46(4), April 2003.

[19] Facebook. "Accessing Your Facbook Info." Web. 10 October 2012. <https://www.facebook.com/help/326826564067688>.

[20] Federal Trade Commission. "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, FTC Report." March 2012. Web. 8 November 2013. <http://ftc.gov/os/2012/03/120326privacyreport.pdf>.

[21] Fictionwise LLC. "Overdrive and the eReader Replacement File Program." Web. 13 October 2012. <http://mobile.fictionwise.com/servlet/mw?t=help_Overdrive-Replacement-Faq.htm>.

[22] E.W. Felten. "A Skeptical View of DRM and Fair Use." *Communications of the ACM*, 46(4): 56-61, April 2003.

[23] E.W. Felten. "DRM and Public Policy." *Communications of the ACM*, 48(7): 112, July 2005.

[24] E.W. Felten. "Understanding Trusted Computing: Will its Benefits Outweigh its Drawbacks?" *IEEE Security and Privacy*, May 2003.

[25] E.W. Felten and J.A. Halderman. "Digital Rights Management, Spyware, and Security." *IEEE Security and Privacy*, January/February 2006.

[26] Flurry. "Privacy Policy." Web. 10 October 2012. <http://www.flurry.com/privacy-policy.html>.

[27] Forbrukerombudet. "iTunes Violates Norwegian Law." 6 July 2006. Web. 14 October 2012. <http://www.forbrukerombudet.no/id/11032467.0>.

[28] B.L. Fox and B.A. LaMacchia. "Encouraging Recognition of Fair Uses in DRM Systems." *Communications of the ACM*, 46(4), April 2003.

[29] D. Goodin. "Backdoor in Top iPhone Games Stole User Data, Suit Claims." The Register. 6 November 2009. Web. 10 November 2013. <http://www.theregister.co.uk/2009/11/06/iphone_games_storm8_lawsuit/>.

[30] G. GreenLeaf. "APEC's Privacy Framework Sets a New Low Standard for the Asia-Pacific." New Dimensions in Privacy Law: International and Comparative Perspectives. Eds. A.T. Kenyon and M. Richardson. New York: Cambridge University Press, 2006. 91-120. Print.

[31] J.A. Halderman and E.W. Felten. "Lessons from the Sony CD DRM Episode." *USENIX Security Symposium*, August 2006.

[32] J. Hess. "Palm Pre Privacy." Joey Hess. Web. 10 October 2012. <http://joeyh.name/blog/entry/Palm_Pre_privacy/>.

[33] P. Higgins. "A Better Path for Apps: Respecting Users and Their Privacy." Electronic Frontier Foundation. 8 February 2012. Web. 8 November 2013. <https://www.eff.org/deeplinks/2012/02/better-path-apps-respecting-users-and-their-privacy>.

[34] P. Higgins. "Highlighting a Privacy Problem: Apps Need to Respect User Rights From the Start." Electronic Frontier Foundation. 8 March 2012. Web. 8 November 2013. <https://www.eff.org/deeplinks/2012/03/highlighting-privacy-problems-apps-need-respect-user-rights-start>.

[35] P. Higgins. "Mobile User Privacy Bill of Rights." Electronic Frontier Foundation. 2 March 2012. Web. 8 November 2013. <https://www.eff.org/deeplinks/2012/03/best-practices-respect-mobile-user-bill-rights>.

[36] P. Higgins and L. Tien. "EFF to FCC: Consumers Face Uphill Battle in Fight for Mobile Device Privacy." Electronic Frontier Foundation. 16 July 2012. Web. 8 November 2013. <https://www.eff.org/deeplinks/2012/07/eff-fcc-consumers-face-uphill-battle-fight-mobile-device-privacy>.

[37] P. Higgins and L. Tien. "Privacy and Security of Information Stored on Mobile Communications Devices: CC Docket No. 96-115; DA 12-818 (77 Fed. Reg. 35336)." Electronic Frontier Foundation. 13 July 2012. Web. 8 November 2013. <https://www.eff.org/files/EFF%20FCC%20Mobile%20Privacy%20Comments.pdf>.

[38] P. Higgins and R. Reitman. "California AG Agreement Calls on Mobile Apps to Be Transparent About All the Ways They Invade User Privacy." Electronic Frontier Foundation. 23 February 2012. Web. 8 November 2013. <https://www.eff.org/deeplinks/2012/02/california-ag-agreement-calls-mobile-apps-be-transparent-about-all-ways-they>.

[39] M. Hofmann. "Carrier IQ Tries to Censor Research With Baseless Legal Threat." Electronic Frontier Foundation. 21 November 2011. Web. 8 November 2013. <https://www.eff.org/deeplinks/2011/11/carrieriq-censor-research-baseless-legal-threat>.

[40] M. Hofmann. "Obama Administration Unveils Promising Consumer Privacy Plan, but the Devil Will Be in the Details." Electronic Frontier Foundation. 23 February 2012. Web. 8 November 2013. <https://www.eff.org/deeplinks/2012/02/obama-administration-unveils-promising-consumer-privacy-plan-devil-details>.

[41] H. Holtmann. "Is Big Brother Listening in on Many iPhone Apps?" Eidac. 10 March 2009. Web. 30 November 2012. <http://www.eidac.de/?p=109>.

[42] L. Lessig. Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity. *The Penguin Press*, 348 pages, 2004.

[43] L. Lessig. Code Version 2.0. New York: *Basic Books*, 410 pages, 2006.

[44] Library of Congress. "Bill Text 108th Congress (2003-2004) H.R.107.IH." Web. 14 November 2013. <http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.107:>.

[45] Library of Congress. "Bill Text 108th Congress (2003-2004) S.1621.IS." Web. 11 October 2012. <http://thomas.loc.gov/cgi-bin/query/z?c108:s1621:>.

[46] Library of Congress. "Bill Text Versions 105th Congress (1997-1998) H.R.2281." Web. 11 October 2012. <http://thomas.loc.gov/cgi-bin/query/z?c105:H.R.2281:>.

[47] Library of Congress. "Bill Text 105th Congress (1997-1998) H.R.3048.IH." Web. 11 October 2012. <http://thomas.loc.gov/cgi-bin/query/z?c105:H.R.3048:>.

[48] Library of Congress. "Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies." 26 October 2012. Web. 31 October 2013. <http://www.copyright.gov/fedreg/2012/77fr65260.pdf.

[49] D. Lindsay and S. Ricketson. "Copyright, Privacy, and Digital Rights Management (DRM)." New Dimensions in Privacy Law: International and Comparative Perspectives. Eds. A.T. Kenyon and M. Richardson. New York: Cambridge University Press, 2006. 121-153. Print.

[50] N. Lucchi. "Countering the Unfair Play of DRM Technologies." *Texas Intellectual Property Law Journal*, 16(1): 91-123, 2007.

[51] V. Mayer-Shönberger. "Beyond Copyright: Managing Information Rights with DRM." *Denver University Law Review*, 84(1): 181-198, 2007.

[52] G. Mazziotti. EU Digital Copyright Law and the End-User, Chapter 7: Freedom of Use vs. DRM Technology. *Springer*, pages 179-229, 2008.

[53] Medialets. "Welcome to Muse." Web. 11 November 2013. <http://muse.medialets.com>.

[54] Mobclix. "Analytics." Web. 11 November 2013. <http://www.mobclix.com/faqs.html#faqs-4>.

[55] D. Morin. "We are sorry." Path. 8 February 2012. Web. 10 October 2012. <http://blog.path.com/post/17274932484/we-are-sorry>.

[56] Office of the Attorney General. "Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications." State of California Department of Justice. 22 February 2012. Web. 8 November 2013. <http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy>.

[57] K. Opsahl. "A Bill of Privacy Rights for Social Network Users." Electronic Frontier Foundation. 19 May 2010. Web. 8 November 2013. <https://www.eff.org/deeplinks/2010/05/bill-privacy-rights-social-network-users>.

[58] The Organisation for Economic Co-operation and Development. "30 Years After: the Impact of the OECD Privacy Guidelines." 10 March 2010. Web. 14 November 2013. <http://www.oecd.org/sti/ieconomy/30yearsaftertheimpactoftheoecdprivacyguidelines.htm>.

[59] The Organisation for Economic Co-operation and Development (OECD). "OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data." *OECD.* C(80)58/FINAL, 11 July 2013. Web. 7 September 2013. <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>.

[60] 0th3lo. "Pinchmedia: The Anatomy of a Spyware Vendor." 31 July 2009. Web. 10 November 2013. <http://archive-i-phone-home.blogspot.com/2009/07/pinchmedia-anatomy-of-spyware-vendor.html>.

[61] N.A. Ozer. "Note to Self: Siri Not Just Working for Me, Working Full-Time for Apple, Too." American Civil Liberties Union of Northern California. 12 March 2012. Web. 1 March 1013. <https://www.aclunc.org/blog/note-self-siri-not-just-working-me-working-full-time-apple-too>.

[62] PayPal, Inc. "Amendment to the PayPal User Agreement and Privacy Policy, Effective Date: Nov 01, 2012." Web. 14 October 2012. <https://cms.paypal.com/us/cgi-bin/?cmd=_render-content&content_ID=ua/US_20121001_Amendment_to_UA_and_Privacy_print&fli=true&locale.x=en_US,>.

[63] S. Perez. "Dear iPhone Users: Your Apps Are Spying on You." The New York Times. 17 August 2009. Web. 10 November 2013. <http://www.nytimes.com/external/readwriteweb/2009/08/17/17readwriteweb-dear-iphone-users-your-apps-are-spying-on-y-42589.html>.

[64] N. Perlroth and N. Bilton. "An Easy Sweep of User Data from Devices." The New York Times. 16 February 2012. Web. 10 November 2013. <http://query.nytimes.com/gst/fullpage.html?res=9B07E4D7163FF935A25751C0A9649D8B63>.

[65] J.T. Rosch. "Keynote Address: A Different Perspective on DRM." *Berkeley Technology Law Journal*, 22(3): 971-980, 2007.

[66] B. Rosenblatt. "DRM, Law and Technology: An American Perspective." *Online Information Review*, 31(1): 73-84, 2007.

[67] C. Russell. "Fair Use Under Fire." *Library Journal*, 128(13): 32, August 2003.

[68] P. Samuelson. "DRM {and, or, vs.} the Law." *Communications of the ACM*, 46(4): 41-45, April 2003.

[69] A.C. Sanders. "Restraining Amazon.com's Orwellian Potential: The Computer Fraud and Abuse Act as Consumer Rights Legislation." *Federal Communications Law Journal*, 63(2): 535-552, March 2011.

[70] D.J. Schaffner. "The Digital Millennium Copyright Act: Overextension of Copyright Protection and the Unintended Chilling Effects on Fair Use, Free Speech, and Innovation." *Cornell Journal of Law and Public Policy*, 14(1): 145-170, 2004.

[71] K. Schiller. "A Happy Medium: Ebooks, Licensing, and DRM." *Information Today*, 27(2): 42-44, February 2010.

[72] N. Seriot. “iPhone Privacy.” Black Hat. 2010. Web. 30 November 2012. <http://seriot.ch/resources/talks_papers/iPhonePrivacy.pdf>.

[73] V. Silver. “Spyware Matching FinFisher Can Take Over iPhones.” Bloomberg News. 29 August 2012. Web. 8 November 2013. <http://www.bloomberg.com/news/2012-08-29/spyware-matching-finfisher-can-take-over-iphone-and-blackberry.html>.

[74] Sony Computer Entertainment Inc. “Playstation Vita System Software License Agreement (Version 1.1).” 2011. Web. 13 October 2012. <http://www.scei.co.jp/psvita-eula/psvita_eula_en.html>.

[75] R. Stim. Getting Permission: How To License & Clear Copyrighted Materials Online & Off. Berkeley, Calif: *Nolo.com, 2000. Ebook Collection (EBSCOhost).* Web. 31 October 2013.

[76] A. Thampi. “Path Uploads Your Entire iPhone Address Book to its Servers.” Mclov.in. 8 February 2012. Web. 8 November 2013. <http://mclov.in/2012/02/08/path-uploads-your-entire-address-book-to-their-servers.html>.

[77] S. Thurm and Y.I. Kane. “Your Apps Are Watching You: A WSJ Investigation Finds That iPhone and Android Apps Are Breaching the Privacy of Smartphone Users.” The Wall Street Journal. 17 December 2010. Web. 8 November 2013. <http://online.wsj.com/news/articles/SB10001424052748704694004576020083703574602>.

[78] J. Turow, D.K. Mulligan, and C.J. Hoofnagle. “Research Report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace.” Berkeley Law, University of California. October 2007. Web. 8 November 2013. <http://www.law.berkeley.edu/files/annenberg_samuelson_advertising.pdf>.

[79] United States Copyright Office. “Copyright Law of the United States of America and Related Laws Contained in Title 17 of the United States Code: Subject Matter and Scope of Copyright, Circular 92.” Circular 92. Web. 31 October 2013. <http://www.copyright.gov/title17/92chap1.html>.

[80] United States Copyright Office. “Copyright Law of the United States of America and Related Laws Contained in Title 17 of the United States Code: Copyright Protection and Management Systems, Circular 92.” Circular 92. Web. 8 September 2012. <http://www.copyright.gov/title17/92chap12.html>.

[81] United States Copyright Office. "Rulemaking on Exemptions from Prohibition on Circumvention of Technological Measures that Control Access to Copyrighted Works." Web. 14 September 2012. <http://www.copyright.gov/1201/2010/>.

[82] United States Copyright Office. "The Digital Millennium Copyright Act of 1998: U.S. Copyright Office Summary." 28 October 1998. Web. 31 October 2013. <http://www.copyright.gov/legislation/dmca.pdf>.

[83] United States Court of Appeals. No. 04-3654: Vivendi Universal, Inc. v. Jung &Crittenden. 20 June 2005. Web. 13 October 2012. <https://www.eff.org/files/filenode/Blizzard_v_bnetd/20050901_decision.pdf>.

[84] United States Court of Appeals, Second Circuit. "Maxtone-Graham v. Burtchaell 803 F.2d 1253." 15 October 1986. Web. 1 November 2013. <http://www.studentweb.law.ttu.edu/cochran/Cases%20&%20Readings/Copyright-UNT/maxtonegraham.htm>.

[85] United States District Court for the District of New Hampshire. "Keep Thomson Governor Committee, Peter Thomson, Chairman, Orford, New Hampshire v. Citizens for Gallen Committee, Virginia Connors, Chairman, and Hugh Gallen." October 1978. Web. 1 November 2013. <http://law.onu.edu/sites/default/files/457_F__Supp __957%28rev%29%28DAK%29.pdf>.

[86] United States Government Accountability Office. "Report to Congressional Requesters: Privacy Alternatives Exist for Enhancing Protection of Personally Identifiable Information." (GAO-08-536). May 2008.

[87] United States Public Policy Committee of the Association for Computing Machinery. "Letter to the Honorable Sam Brownback." February 2004. Web. 14 September 2012. <http://techpolicy.acm.org/blog/?p=17>.

[88] J.M. Urban, C.J. Hoofnagle, and S. Li. "Mobile Phones and Privacy: UC Berkeley Public Law Research Paper No. 2103405." *BCLT Research Paper Series* July 2012.

[89] The Wall Street Journal. "The Journal's Cellphone Testing Methodology." 18 December 2010. Web. 10 November 2013. <http://online.wsj.com/news/articles/SB10001424052748704034804576025951767626460>.

[90] The Wall Street Journal. "What They Know—Mobile." 18 December 2010. Web. 10 November 2013. <http://blogs.wsj.com/wtk-mobile/>.

[91] S.B. Wicker. "The Loss of Location Privacy in the Cellular Age." *Communications of the ACM*, 55(8): 60-68, August 2012.

[92] S.B. Wicker and D.E. Schrader. "Privacy-Aware Design Principles for Information Networks." *Proceedings of the IEEE*, 99(2): 330-350, January 2011.